Axelar Network:

การเชื่อมต่อแอปพลิเคชันกับ Blockchain Ecosystems

Draft 1.0

มกราคม 2021

Abstract

Blockchain ecosystems หลายแห่งกำลังเกิดขึ้นซึ่งมีคุณลักษณะเฉพาะและแตกต่างที่น่าดึงดูดใจให้กับผู้ใช้และนักพัฒนาแอพพลิเคชั่น อย่างไรก็ตาม การสื่อสารทั่วทั้งระบบนิเวศนั้นเบาบางมากและแยกออกจากกัน เพื่อให้แอปพลิเคชันสามารถสื่อสารข้าม blockchain ecosystems ได้อย่างราบรื่น เราขอเสนอ axelar axelar stack มีเชนกระจายอำนาจ โปรโตคอล เครื่องมือ และ api ที่อนุญาตการสื่อสาร cross-chain อย่างง่าย ชุดโปรโตคอล axelar ประกอบด้วยการกำหนดเส้นทางและการถ่ายโอนข้ามพรมแดนโปรโตคอล เชนแบบเปิดที่กระจายอำนาจของผู้ตรวจสอบความถูกต้องจะขับเคลื่อนเชน ทุกคนสามารถเข้าร่วมใช้งานได้และมีส่วนร่วม. ฉันทามติไบแซนไทน์ การเข้ารหัส และกลไกจูงใจได้รับการออกแบบมาเพื่อให้บรรลุเป้าหมายข้อกำหนดด้านความปลอดภัยและความมีชีวิตชีวาเฉพาะสำหรับคำร้องขอ cross-chain

1. บทนำ

ระบบบล็อคเชนกำลังได้รับความนิยมอย่างรวดเร็วและดึงดูดกรณีการใช้งานใหม่ๆ สำหรับการแปลงโทเค็นสินทรัพย์การเงินแบบกระจายอำนาจ และแอปพลิเคชันแบบกระจายอื่นๆ หลายแพลตฟอร์มหลักเช่น Ethereum, Monero,EOS, Cardano, Terra, Cosmos, Avalanche, Algorand, Near, Celo และ Polkadot นำเสนอคุณสมบัติที่แตกต่างและสภาพแวดล้อมการพัฒนา ที่ทำให้น่าสนใจสำหรับการใช้งานที่แตกต่างกัน กรณีการใช้งาน และผู้ใช้ปลายทาง [5, 11, 4, 21, 20, 23, 24, 19, 6, 14, 25] อย่างไรก็ตาม ฟีเจอร์ที่มีประโยชน์ของแพลตฟอร์มใหม่แต่ละแพลตฟอร์มในปัจจุบัน คือ เสนอให้กับผู้ใช้ระบบนิเวศน้อยกว่า 1% กล่าวคือ ผู้ถือโทเค็นดั้งเดิมบนแพลตฟอร์มนั้น เราจะอนุญาตให้นักพัฒนาแพลตฟอร์มเชื่อมต่อบล็อคเชนกับ ระบบนิเวศอื่น ๆ ได้อย่างง่ายดายหรือไม่? เราเปิดใช้งานได้ไหมผู้สร้างแอปพลิเคชันเพื่อสร้างบนแพลตฟอร์มที่ดีที่สุดสำหรับความต้องการของพวกเขา ในขณะที่ยังคงสื่อสารผ่านหลาย ๆ ตัวระบบนิเวศบล็อคเชน เราอนุญาตให้ผู้ใช้โต้ตอบกับแอปพลิเคชันใด ๆ บนบล็อคเชนใด ๆ ได้โดยตรงจากกระเป๋าเงินของพวกเขา

เพื่อเชื่อมโยงระบบนิเวศบล็อกเชนและช่วยให้แอปพลิเคชันสามารถสื่อสารข้ามกันได้เราขอเสนอเชน Axelar เครื่องมือตรวจสอบร่วมกันเรียกใช้โปรโตคอลฉันทามติแบบไบแซนไทน์และเรียกใช้โปรโตคอลอำนวยความสะดวกในการร้องขอ cross-chain ทุกคนสามารถเข้าร่วมเชน เข้าร่วม และใช้งานได้ พื้นฐานเชนได้รับการปรับให้เหมาะสมสำหรับ

ข้อกำหนดด้านความปลอดภัยและความมีชีวิตชีวาสูงซึ่งเป็นเอกลักษณ์เฉพาะสำหรับคำขอ cross-chain Axelar เชนยังรวมถึงชุดโปรโตคอลและ API โปรโตคอลหลักคือ:

- Cross-Chain Gateway Protocol (CGP) โปรโตคอลนี้คล้ายคลึงกับ Border Gateway Protocol บนอินเตอร์เนต โปรโตคอลนี้ใช้เพื่อเชื่อมต่อระบบนิเวศบล็อกเชนแบบอิสระหลายระบบและรับผิดชอบในการกำหนดเส้นทางข้ามระบบนิเวศเหล่านั้น บล็อคเชนไม่จำเป็นต้อง "พูดภาษาที่กำหนดเอง" นักพัฒนาแพลตฟอร์มของพวกเขาไม่จำเป็นต้องทำการเปลี่ยนแปลงใด ๆ ที่กำหนดเองบนเชนของพวกเขา และสามารถเชื่อมต่อเชนเข้ากับเชนทั่วโลกได้อย่างง่ายดาย
- Cross-Chain Transfer Protocol (CTP) โปรโตคอลนี้คล้ายคลึงกับโปรโตคอลระดับแอปพลิเคชัน File Transfer, Hypertext Transfer Protocols บนอินเทอร์เน็ต เป็นสแต็กโปรโตคอลระดับแอปพลิเคชันที่อยู่บนโปรโตคอลการเราต์ (เช่น CGP และเทคโนโลยีการกำหนดเส้นทางอื่นๆ) นักพัฒนาแอพพลิเคชั่น สามารถเชื่อมต่อ dapps ของตนกับ chain ใดก็ได้เพื่อดำเนินการคำขอข้ามสาย ผู้ใช้สามารถใช้โปรโตคอล CTP เพื่อโต้ตอบกับแอปพลิเคชันบนสายใด ๆ โดยใช้การเรียก API แบบง่ายที่คล้ายกับ HTTP GET/POST คำขอ นักพัฒนาสามารถล็อค ปลดล็อค และโอนทรัพย์สินระหว่างที่อยู่สองแห่งบนแพลตฟอร์มบล็อคเชนใด ๆ เรียกใช้งานแอปพลิเคชัน cross-chain (เช่น dapps บนเชน A สามารถอัปเดต 1 สถานะหากแอปพลิเคชันอื่นบนเชน B ตรงตามเกณฑ์การค้นหาบางอย่าง (อัตราดอกเบี้ย > X)) และดำเนินการคำขอ cross-chain ทั่วไประหว่างแอปข้ามเชน (สัญญาอัจฉริยะบนเชน A สามารถโทรได้ เพื่ออัปเดตสถานะของสัญญาอัจฉริยะบนเชน B) โปรโตคอลนี้ช่วยให้สามารถเขียนโปรแกรมได้ทั่วระบบนิเวศบล็อกเชน

เชน Axelar มีข้อดีดังต่อไปนี้:

- สำหรับผู้สร้างแพลตฟอร์มบล็อกเชน: ความสามารถในการเสียบบล็อกเชนกับบล็อกเชนอื่นๆ ทั้งหมดได้อย่างง่ายดายระบบนิเวศ ต้องตั้งค่าบัญชีเกณฑ์เท่านั้นในเชนเพื่อเสียบเข้ากับเชน
- สำหรับผู้สร้าง dapps: ผู้สร้างแอปพลิเคชันสามารถโฮสต์ dapp ของตนได้ทุกที่ ล็อก ปลดล็อก โอนสินทรัพย์และสื่อสารกับแอปพลิเคชันบนสายอื่น ๆ ผ่าน CTP API
- สำหรับผู้ใช้: ผู้ใช้สามารถโต้ตอบกับแอปพลิเคชันทั้งหมดทั่วทั้งระบบนิเวศได้โดยตรงจากกระเป๋าเงินของพวกเขา

แพลตฟอร์มสำหรับผู้สร้าง สุดท้ายนี้ เชน Axelar เป็นแพลตฟอร์มสำหรับนักพัฒนาและชุมชนระดับโลก รูปแบบการกำกับดูแลเปิดให้ทุกคน นักพัฒนาสามารถเสนอจุดบูรณาการใหม่ การกำหนดเส้นทาง และโปรโตคอลระดับแอปพลิเคชัน และผู้ใช้สามารถตัดสินใจได้ว่าจะใช้จุดเหล่านี้หรือไม่โดยลงคะแนนในข้อเสนอ และหากได้รับอนุมัติ ผู้ตรวจสอบจะยอมรับการเปลี่ยนแปลง

1.1. โซลูชันการทำงานร่วมกันที่มีอยู่

ความพยายามครั้งก่อนในการแก้ปัญหาการทำงานร่วมกันข้ามบล็อคเชนนั้นจัดเป็นหนึ่งในสี่ประเภท: การแลกเปลี่ยนแบบรวมศูนย์ ระบบนิเวศที่ทำงานร่วมกันได้ สินทรัพย์ที่ห่อหุ้ม และสะพานโทเค็น เราสรุปแนวทางเหล่านี้โดยย่อด้านล่าง

ระบบจากส่วนกลาง (Centralized Systems) ทุกวันนี้ ระบบจากส่วนกลางเป็นโซลูชันเดียวที่ปรับขนาดได้อย่างแท้จริงสำหรับความต้องการด้านการทำงานร่วมกันสำหรับระบบนิเวศ พวกเขาสามารถแสดงรายการสินทรัพย์หรือบนแพลตฟอร์มใด ๆ ได้อย่างง่ายดาย อย่างไรก็ตาม เป็นที่ทราบกันดีว่าระบบจากส่วนกลางมีปัญหาด้านความปลอดภัยต่างๆ และไม่ดีพอที่จะขับเคลื่อนระบบการเงินแบบกระจายศูนย์ซึ่งต้องการความปลอดภัยที่แข็งแกร่ง ความโปร่งใส และการกำกับดูแลแบบเปิด ด้วยตัวของมันเอง พวกเขาไม่สามารถขับเคลื่อนแอพพลิเคชันแบบกระจายอำนาจได้เมื่อเติบโตขึ้น

ฮับการทำงานร่วมกัน (Interoperability Hubs) โครงการต่าง ๆ เช่น Cosmos, Polkadot, Ava labs กล่าวถึงการทำงานร่วมกันระหว่าง sidechains ที่มีถิ่นกำเนิดในระบบนิเวศของพวกเขาโดยใช้โปรโตคอลการสื่อสารระหว่างห่วงโซ่ที่กำหนดเอง [23, 25, 24] ตัวอย่างเช่นหนึ่งสามารถหมุนขึ้นเก้าอี้ข้าง (โซนคอสมอส) ที่สามารถสื่อสารกับฮับจักรวาล เก้าอี้ด้านข้างจะต้องขึ้นอยู่กับฉันทามติ Tendermint และพูดโปรโตคอลที่เข้าใจโดยกำเนิดโดยศูนย์กลางจักรวาล การเชื่อมต่อกับบล็อกเชนและระบบนิเวศอื่น ๆ ที่พูดภาษาต่าง ๆ ถูกทิ้งไว้ที่เทคโนโลยีภายนอก

สะพานคู่ (Pairwise Bridges) สินทรัพย์ที่ถูกห่อหุ้ม (เช่น wrapped Bitcoins) พยายามเติมช่องว่างการทำงานร่วมกันข้ามห่วงโซ่ที่ขาดหายไปในระบบนิเวศ ตัวอย่างหนึ่งคือ tBTC [9] ซึ่งเป็นโปรโตคอลที่กำหนดเองซึ่งมีการใช้สัญญาอัจฉริยะและหลักประกันอย่างชาญฉลาดเพื่อรักษาความปลอดภัยในการถ่ายโอน โซลูชันเหล่านี้ต้องใช้ความพยายามทางวิศวกรรมอย่างมากในการสร้าง – สำหรับแต่ละคู่ห่วงโซ่นักพัฒนาจะต้องสร้างสัญญาอัจฉริยะใหม่ในห่วงโซ่ปลายทางที่แยกวิเคราะห์หลักฐานสถานะจากห่วงโซ่ต้นทาง (คล้ายกับที่แต่ละห่วงโซ่ด้านข้างสามารถแยกวิเคราะห์สถานะของห่วงโซ่อื่น ๆ ได้อย่างไร) มีสะพานเพียงไม่กี่แห่งเท่านั้นที่ถูกนำมาใช้โดยใช้วิธีนี้ วิธีการเหล่านี้ไม่ได้ปรับขนาดเมื่อหนึ่งในบล็อกเชนพื้นฐานต้องการอัพเกรดกฎฉันทามติหรือรูปแบบการทำธุรกรรม นี่เป็นเพราะสัญญาอัจฉริยะทั้งหมดที่ขึ้นอยู่กับสถานะของห่วงโซ่เหล่านี้จะต้องได้รับการอัพเกรด เราต้องตั้งค่าตัวตรวจสอบความถูกต้องและกำหนดให้พวกเขาล็อคสินทรัพย์ที่แตกต่างกันเพื่อปกปิดการถ่ายโอนสินทรัพย์ใด ๆ ซึ่ง จำกัด ประสิทธิภาพทางเศรษฐกิจของการถ่ายโอนดังกล่าว

นอกจากนี้เรายังได้เห็นสะพานวัตถุประสงค์เดียวอื่นๆ อีกสองสามแห่งโดยนักพัฒนาแพลตฟอร์มที่เขียนตรรกะการเปลี่ยนสถานะใหม่ในสัญญาอัจฉริยะเพื่อเชื่อมโยงไปยังระบบนิเวศอื่นๆ [1, 7] พวกเขาประสบปัญหาด้านความสามารถในการปรับขยายได้หลายอย่าง ไม่อนุญาตให้ระบบนิเวศปรับขนาดได้อย่างสม่ำเสมอ และแนะนำการพึ่งพาเพิ่มเติมสำหรับแอปพลิเคชัน ตัวอย่างเช่น หากแพลตฟอร์มใดแพลตฟอร์ม

หนึ่งเปลี่ยนแปลง สัญญาอัจฉริยะทั้งหมดบนบริดจ์ทั้งหมดจะต้องได้รับการอัปเกรด ในที่สุด 2 คนนี้จะทำให้ระบบนิเวศอยู่ในกริดล็อคที่ไม่มีใครสามารถอัพเกรดได้ สุดท้าย หากบริดจ์วัตถุประสงค์เดียวเชื่อมต่อแพลตฟอร์ม A และ B และบริดจ์วัตถุประสงค์เดียวที่สองเชื่อมต่อ B และ C ไม่ได้หมายความว่าแอปพลิเคชันบน A จะสามารถพูดคุยกับแอปพลิเคชันบน C ได้ หนึ่งอาจต้องสร้างอีกอัน บริดจ์เอนกประสงค์หรือลอจิกแอปพลิเคชัน rewire

ความพยายามอื่น ๆ ในการจัดการกับการทำงานร่วมกัน ได้แก่ oracles แบบติดต่อกับภายนอก (เช่น Ren [8]) และบล็อกเชนที่ทำงานร่วมกันเฉพาะแอปพลิเคชัน [10]

เพื่อสรุปโซลูชันที่มีอยู่สำหรับการทำงานร่วมกันต้องทำงานวิศวกรรมหนักจากทั้งนักพัฒนาแพลตฟอร์มและผู้สร้างแอปพลิเคชันที่ต้องเข้าใจโปรโตคอลการสื่อสารที่แตกต่างกันเพื่อสื่อสารในระบบนิเวศทุกคู่ ดังนั้นการทำงานร่วมกันจึงแทบไม่มีอยู่ในพื้นที่บล็อกเชนในปัจจุบัน ในตอนท้ายของวันนักพัฒนาแพลตฟอร์มต้องการมุ่งเน้นไปที่การสร้างแพลตฟอร์มและเพิ่มประสิทธิภาพสำหรับกรณีการใช้งานและสามารถเชื่อมต่อกับบล็อกเชนอื่น ๆ ได้อย่างง่ายดาย และนักพัฒนาแอปพลิเคชันต้องการสร้าง dapps บนแพลตฟอร์มที่ดีที่สุดสำหรับความต้องการของพวกเขาในขณะที่ยังคงใช้ประโยชน์จากผู้ใช้สภาพคล่องและสื่อสารกับ dapps อื่น ๆ ในห่วงโซ่อื่น ๆ

2. การแสวงหาการสื่อสารข้ามห่วงโซ่ที่ปรับขนาดได้

แกนหลักการสื่อสาร cross-chain ต้องการให้เชนที่ต่างกันค้นหาความสามารถในการสื่อสาร โดยใช้ภาษาเดียวกัน เพื่อแก้ปัญหานี้ เราอธิบายชุดโปรโตคอล Axelar อธิบายคุณสมบัติระดับสูง และอธิบายว่าคุณสมบัติเหล่านี้จัดการกับแกนกลางของการสื่อสารข้ามสายที่ปรับขนาดได้อย่างไร

1. การผสานรวม "Plug-and-play" ผู้สร้างแพลตฟอร์มบล็อคเชนไม่จำเป็นต้องทำงานหนักงานวิศวกรรมหรือบูรณาการเพื่อพูด "ภาษาที่กำหนดเอง" เพื่อรองรับการข้ามสาย โปรโตคอล cross-chain ควรจะสามารถเชื่อมต่อ blockchain ที่มีอยู่หรือใหม่ได้โดยไม่เสียดสี สินทรัพย์ใหม่ควรเพิ่มด้วยความพยายามเพียงเล็กน้อย
2. การกำหนดเส้นทาง cross-chain ฟังก์ชันต่างๆ เช่น การค้นหาที่อยู่เชน เส้นทางเส้นทาง และเชนเป็นแกนหลักของอินเทอร์เน็ตและอำนวยความสะดวกโดย BGP และโปรโตคอลการกำหนดเส้นทางอื่นๆ ในทำนองเดียวกันถึงอำนวยความสะดวกในการสื่อสารข้ามระบบนิเวศบล็อคเชน เราจำเป็นต้องสนับสนุนการค้นพบที่อยู่ทั้งแอปพลิเคชันและการกำหนดเส้นทาง
3. รองรับการอัพเกรด หากระบบนิเวศของบล็อคเชนเปลี่ยนแปลงไป ก็ไม่ควรส่งผลกระทบต่อการทำงานร่วมกันของบล็อคเชนอื่นๆ ระบบจำเป็นต้องรับรู้การอัพเดต และความพยายามน้อยที่สุดควรเป็นจำเป็นเพื่อรองรับพวกเขา (กล่าวคือ ไม่ควรเขียน "ตรรกะการเปลี่ยนสถานะ" ใหม่ และแอปพลิเคชันควรไม่แตก)
4. ภาษาสม่ำเสมอในการสมัคร แอปพลิเคชันต้องการโปรโตคอลง่ายๆ ในการล็อก ปลดล็อก ถ่ายโอน และสื่อสารกับแอปพลิเคชันอื่น ๆ ไม่ว่าพวกเขาจะอยู่บนสายใด โปรโตคอลนี้จะต้องchain-agnostic

และรองรับการเรียกง่ายๆ คล้ายกับโปรโตคอล HTTP/HTTPS ที่อนุญาตให้ผู้ใช้และเบราว์เซอร์เพื่อสื่อสารกับเว็บเซิร์ฟเวอร์ใด ๆ เมื่อมีเชนและสินทรัพย์เข้าร่วมการกำหนดเส้นทางระดับล่างมากขึ้นโปรโตคอลแอปพลิเคชันควรจะใช้สำหรับการสื่อสารโดยไม่ต้องเขียนซอฟต์แวร์ใหม่กอง

ต่อไป เราจะสรุปข้อกำหนดด้านความปลอดภัยที่โปรโตคอลเหล่านี้ต้องปฏิบัติตาม

1. *ความไว้วางใจแบบกระจายอำนาจ* เชนและโปรโตคอลต้องมีการกระจายอำนาจ เปิดกว้าง และอนุญาตให้ทุกคนมีส่วนร่วมอย่างเป็นธรรม
2. *ความปลอดภัยสูง* ระบบต้องเป็นไปตามการรับประกันความปลอดภัยสูง ระบบจำเป็นต้องรักษาความปลอดภัยของสินทรัพย์และสถานะในขณะที่เชน cross-chain ประมวลผล
3. *ความมีชีวิตชีวาสูง* ระบบจะต้องตอบสนองการค้ำประกันความมีชีวิตชีวาสูง เพื่อรองรับแอพพลิเคชั่นที่ใช้ประโยชน์จากคุณสมบัติ cross-chain

การตอบสนองบางส่วนของคุณสมบัติเหล่านี้เป็นเรื่องง่าย ตัวอย่างเช่น หนึ่งสามารถสร้างบัญชี multisig แบบรวมศูนย์ได้กับเพื่อน ๆ และล็อค / ปลดล็อคทรัพย์สินในเครือที่เกี่ยวข้อง ระบบดังกล่าวมีความเสี่ยงโดยเนื้อแท้เพื่อการสมรู้ร่วมคิดและการโจมตีเซ็นเซอร์ และขาดแรงจูงใจที่เหมาะสมสำหรับ ผู้ตรวจสอบความถูกต้องเพื่อปกป้องพวกเขา การสร้างชุดเชนและโปรโตคอลที่กระจายอำนาจซึ่งทุกคน สามารถเข้าร่วมได้ในขณะที่ได้รับแรงจูงใจอย่างถูกต้องสามารถเปิดใช้งานการสื่อสาร cross-chain ที่ลื่นไหล แต่การแก้ปัญหาเป็นปัญหาที่ยากที่ต้องใช้ความระมัดระวังการรวมกันของฉันทามติ การเข้ารหัสลับ และโปรโตคอลการออกแบบกลไก

3. Axelar Network

เชน Axelar มอบโซลูชันที่เป็นหนึ่งเดียวสำหรับการสื่อสาร cross-chain ที่ตอบสนองความต้องการของนักพัฒนาแพลตฟอร์มทั้งสอง – ไม่จำเป็นต้องมีการผสานรวมจากพวกเขา และผู้สร้างแอปพลิเคชัน – โปรโตคอลง่ายๆ เพียงหนึ่งเดียวและ API เพื่อเข้าถึงสภาพคล่องทั่วโลกและสื่อสารกับระบบนิเวศทั้งหมด

เชน Axelar ประกอบด้วยเชนกระจายอำนาจซึ่งเชื่อมโยงระบบนิเวศบล็อกเชนที่พูดภาษาต่างๆ และชุดโปรโตคอลที่มี API อยู่ด้านบน ทำให้แอปพลิเคชันดำเนินการข้ามสายได้ง่ายคำขอ เชนเชื่อมต่อบล็อคเชนแบบสแตนด์อโลนที่มีอยู่ เช่น Bitcoin, Stellar, Terra, Algorand,และฮับการทำงานร่วมกัน เช่น โซลูชันเช่น Cosmos, Avalanche, Ethereum และ Polkadot ภารกิจของเราคือการช่วยให้นักพัฒนา แอปพลิเคชันสร้างแอปดังกล่าวได้ง่ายขึ้นโดยใช้โปรโตคอลสากลและ API โดยไม่ต้องใช้เปิดตัวโปรโตคอล cross-chain ที่เป็นกรรมสิทธิ์ของตนภายใต้หรือเขียนแอปพลิเคชันใหม่เป็นบริดจ์ใหม่ที่พัฒนา ในการนี้ เราออกแบบชุดโปรโตคอลที่รวมโปรโตคอลเกตเวย์ข้ามสาย (ดูส่วนที่ 6) และ Cross-Chain Transfer Protocol (ดูส่วนที่ 7)

องค์ประกอบหลักของเชนคือโปรโตคอลกระจายอำนาจพื้นฐาน ผู้ตรวจสอบร่วมกันรักษาเชน Axelar และเรียกใช้โหนดที่รักษาความปลอดภัย Axelar blockchain พวกเขาได้รับเลือกผ่านกระบวนการมอบอำนาจโดยผู้ใช้ ผู้ตรวจสอบความถูกต้องจะได้รับอำนาจการลงคะแนนตามสัดส่วนตามสัดส่วนการถือหุ้นถึงพวกเขา ผู้ตรวจสอบความถูกต้องเข้าถึงฉันทามติเกี่ยวกับสถานะของบล็อกเชนหลายตัวที่แพลตฟอร์มเชื่อมต่ออยู่ถึง บล็อกเชนมีหน้าที่ดูแลและเรียกใช้โปรโตคอลการกำหนดเส้นทางและการถ่ายโอน cross-chain กฎการกำกับดูแลช่วย ให้ผู้เข้าร่วมเชนสามารถตัดสินใจเกี่ยวกับโปรโตคอลได้ เช่น บล็อกเชนใดที่จะเชื่อมโยงและทรัพย์สินที่จะสนับสนุน

Axelar blockchain เป็นไปตามรูปแบบ Delegated Proof-of-Stake (DPoS) ที่คล้ายกับ Cosmos Hub ผู้ใช้เลือกผู้ตรวจสอบความถูกต้องซึ่งต้องผูกมัดเงินเดิมพันของตนเพื่อเข้าร่วมในฉันทามติและรักษาบริการคุณภาพสูง ดิโมเดล DPoS ช่วยให้สามารถบำรุงรักษาชุดตัวตรวจสอบความถูกต้องแบบกระจายศูนย์ขนาดใหญ่ และสิ่งจูงใจที่แข็งแกร่งเพื่อรับประกันว่าผู้ตรวจสอบความถูกต้องมีหน้าที่รับผิดชอบในการบำรุงรักษาบริดจ์และส่วนแบ่งของโครงร่างขีดจำกัดการเข้ารหัส เนื่องจากส่วนหนึ่งของฉันทามติ ผู้ตรวจสอบความถูกต้องเรียกใช้ซอฟต์แวร์ light-client ของ blockchain อื่น ๆ ทำให้สามารถตรวจสอบสถานะได้ของบล็อคเชนอื่นๆ ผู้ตรวจสอบความถูกต้องรายงานสถานะเหล่านี้ไปยัง Axelar blockchain และครั้งเดียวเพียงพอรายงานสถานะของ Bitcoin, Ethereum และเชนอื่น ๆ ถูกบันทึกไว้ใน Axelar

ต่อจากนั้น ชั้นฐานของ Axelar จะรับรู้ถึงสถานะของบล็อคเชนภายนอกได้ตลอดเวลาการสร้าง "สะพานขาเข้า" จากบล็อคเชนอื่น ๆ ผู้ตรวจสอบจะร่วมกันรักษาบัญชีลายเซ็นเกณฑ์บนบล็อคเชนอื่น ๆ (เช่น 80% ของผู้ตรวจสอบต้องอนุมัติและลงนามในธุรกรรมใด ๆนอกนั้น) ซึ่งช่วยให้พวกเขาสามารถล็อค และปลดล็อคทรัพย์สินและสถานะข้ามเชนและโพสต์สถานะบนอื่น ๆ blockchains "สะพานขาออก" โดยรวมแล้ว เราสามารถดูเชน Axelar ว่าเป็น Oracle แบบอ่าน/เขียนแบบกระจายอำนาจ

ส่วนที่เหลือของเอกสารจะอธิบายเบื้องต้นและส่วนประกอบเบื้องหลังเซน (ส่วนที่ 4) รายละเอียดทางเทคนิคบางอย่างของเซน (ส่วนที่ 5) โปรโตคอลเกตเวย์ข้ามสาย (ส่วนที่ 6) และโปรโตคอลการถ่ายโอน cross-chain (ส่วนที่ 7)

4. เบื้องต้น (Preliminaries)

4.1. สัญกรณ์และสมมติฐาน

ให้ V(R) หมายถึงชุดของตัวตรวจสอบ Axelar ที่รอบ R ตัวตรวจสอบความถูกต้องแต่ละคนมีน้ำหนัก ตัวเลขเป็น (0, 1]แสดงถึงอำนาจการลงคะแนนของผู้ตรวจสอบนั้น น้ำหนักของเครื่องมือตรวจสอบทั้งหมดรวมกันเป็น 1 เครื่องตรวจสอบความถูกต้องถูกต้องหากเธอเรียกใช้โหนดที่สอดคล้องกับกฎของโปรโตคอล Axelar เพื่อจบบล็อกหรือในการลงนามคำขอ cross-chain Axelar ต้องการเครื่องมือตรวจสอบน้ำหนักรวมที่ถูกต้อง > F เราเรียกพารามิเตอร์F $\in$ [0.5, 1] เกณฑ์โปรโตคอล

Axelar สามารถใช้บล็อกเชน Delegated-Proof-of-Stake ขั้นสุดท้ายในทันที ผู้ตรวจสอบความถูกต้องเรียกใช้ฉันทามติ Byzantine Fault Tolerant (BFT) ในแต่ละรอบ i เพื่อสิ้นสุดบล็อก ith เมื่อบล็อก ith เสร็จสิ้นแล้วฉันทามติ BFT ใหม่ดำเนินการเพื่อจบบล็อก i + 1 เป็นต้น ผู้ตรวจสอบความถูกต้องจะถูกเลือกผ่านตัวแทนเดิมพัน ผู้ใช้ที่มีเงินเดิมพันบางส่วนอาจเลือกที่จะเรียกใช้โหนดตรวจสอบหรือมอบอำนาจการลงคะแนนของพวกเขา(เดิมพัน) ให้กับผู้ตรวจสอบที่มีอยู่ซึ่งลงคะแนนในนามของพวกเขา ชุดตรวจสอบสามารถอัปเดตได้ validatorsเข้าร่วม / ออกจากชุดและผู้ใช้มอบหมาย / ยกเลิกการมอบอำนาจการลงคะแนนของพวกเขา

บล็อกเชนที่แตกต่างกันทำงานภายใต้สมมติฐานเชนที่แตกต่างกัน การสื่อสารแบบซิงโครนัสหมายถึงว่ามีขอบเขตบนคงที่ Δ เกี่ยวกับเวลาที่ใช้ในการส่งข้อความ โดยที่ Δ เป็นที่รู้จักและสามารถถูกสร้างไว้ในโปรโตคอล การสื่อสารแบบอะซิงโครนัสหมายความว่าข้อความอาจใช้เวลานานถึงถูกส่งมอบ และเป็นที่ทราบกันดีว่าโปรโตคอล BFT ไม่สามารถสร้างสำหรับเชนแบบอะซิงโครนัสได้แม้ในมีตัวตรวจสอบที่เป็นอันตรายเพียงตัวเดียว การประนีประนอมที่สมจริงระหว่างซิงโครไนซ์และอะซิงโครนัสคือสมมติฐานของการสื่อสารแบบซิงโครนัสบางส่วน เชนอาจจะอะซิงโครนัสอย่างสมบูรณ์จนถึงเวลาการรักษาเสถียรภาพทั่วโลกที่ไม่รู้จัก (GST) แต่หลังจากการสื่อสาร GST จะซิงโครไนซ์กับaรู้จักขอบเขตบน Δ [17].

บล็อคเชนทั่วไปทำงานภายใต้สมมติฐานของ > F ตัวตรวจสอบความถูกต้อง สำหรับเชนซิงโครนัสโดยทั่วไปแล้ว F = 1/2 จะถูกตั้งค่า แต่สำหรับสมมติฐานที่อ่อนแอกว่าของเชนซิงโครนัสบางส่วน F = 2/3Bitcoin, ส้อมของมัน และ Ethereum เวอร์ชัน Proof-of-Work ปัจจุบันใช้งานได้เฉพาะการซิงโครไนซ์เท่านั้น คนอื่นเช่น Algorand และ Cosmos ต้องการการซิงโครไนซ์เพียงบางส่วนเท่านั้น เมื่อต่อโซ่ผ่าน Axelarการเชื่อมต่อทำงานโดยสมมุติฐานเชนที่แข็งแกร่งที่สุดจากเชนเหล่านี้ ซึ่งตรงกันในกรณีเชื่อมต่อ Bitcoin และ Cosmos เป็นต้น Axelar blockchain นั้นทำงานได้บางส่วนการตั้งค่าแบบซิงโครนัสจึงต้องใช้ F = 2/3 แต่เป็นไปได้ที่จะปรับปรุงข้อกำหนดของเกณฑ์โดยสมมติว่าบล็อกเชนอื่นๆ ที่มีอยู่มีความปลอดภัยและใช้ประโยชน์จากความปลอดภัย

4.2. การเข้ารหัสเบื้องต้นเบื้องต้น (Cryptographic Preliminaries)

ลายเซ็นดิจิทัล (Digital Signatures) รูปแบบลายเซ็นดิจิทัลเป็นชุดของอัลกอริทึม (Keygen, Sign, Verify) Keygen ส่งออกคีย์คู่ (PK, SK) มีเพียงเจ้าของ SK เท่านั้นที่สามารถลงนามในข้อความ แต่ทุกคนสามารถยืนยันลายเซ็นที่ได้รับคีย์สาธารณะ PK ระบบบล็อคเชนส่วนใหญ่ในปัจจุบันใช้ลายเซ็นมาตรฐานอย่างใดอย่างหนึ่งรูปแบบต่างๆ เช่น ECDSA, Ed25519 หรือรูปแบบอื่นๆ [2, 3]

เกณฑ์ลายเซ็น (Threshold Signatures) โครงการลายเซ็นเกณฑ์ช่วยให้กลุ่มของ n ฝ่ายแยกคีย์ลับสำหรับรูปแบบลายเซ็นในลักษณะที่ชุดย่อยของ t + 1 หรือมากกว่าฝ่ายใดสามารถ ทำงานร่วมกันเพื่อสร้างลายเซ็น แต่ไม่มีกลุ่มย่อยของ t หรือน้อยกว่าสามารถสร้างได้ ลายเซ็นหรือแม้กระทั่งเรียนรู้ข้อมูลใด ๆ เกี่ยวกับรหัสลับ ลายเซ็นที่สร้างโดยโปรโตคอลขีดจำกัดสำหรับ ECDSA และ EdDSA มีลักษณะเหมือนกันกับลายเซ็นที่สร้างโดยอัลกอริธึมแบบสแตนด์อโลน

โครงร่างลายเซ็นธรณีประตูแทนที่อัลกอริธึม Keygen และ Sign สำหรับโครงร่างลายเซ็นธรรมดาด้วยโปรโตคอล n-party แบบกระจาย T.Keygen, T.Sign โปรโตคอลเหล่านี้มักต้องการทั้งสาธารณะ ช่องออกอากาศและช่องคู่ส่วนตัวระหว่างฝ่ายต่างๆ และโดยทั่วไปจะมีหลายรอบของการสื่อสาร หลังจากเสร็จสิ้น T.Keygen ผู้ใช้แต่ละรายจะถือส่วนแบ่ง si ของรหัสลับ SKและคีย์สาธารณะ PK ที่เกี่ยวข้อง โปรโตคอล T.Sign อนุญาตให้ฝ่ายเหล่านี้สร้างลายเซ็นสำหรับ a 5 ให้ข้อความที่ถูกต้องภายใต้คีย์สาธารณะ PK ใครก็ตามที่ใช้ Verify . ตรวจสอบลายเซ็นนี้อัลกอริทึมของรูปแบบลายเซ็นดั้งเดิม

4.3. คุณสมบัติของเกณฑ์ลายเซ็น (Properties of Threshold Signatures)

มีคุณสมบัติหลายอย่างที่โครงร่างเกณฑ์อาจมีที่ต้องการเป็นพิเศษสำหรับการกระจายอำนาจเชน:

การรักษาความปลอดภัยจากเสียงข้างมากที่ไม่ซื่อสัตย์ โครงร่างธรณีประตูบางแบบมีข้อจำกัดว่าปลอดภัยเฉพาะเมื่อฝ่าย n ส่วนใหญ่มีความซื่อสัตย์เท่านั้น ดังนั้นพารามิเตอร์ขีดจำกัด t ต้องน้อยกว่ามากกว่า n/2 [15] ข้อจำกัดนี้มักจะมาพร้อมกับความจริงที่ว่า 2t + 1 บุคคลที่ซื่อสัตย์เป็นจำเป็นต้องลงนามแม้ว่าจะมีเพียงฝ่ายที่เสียหายเพียง t + 1 เท่านั้นที่สามารถสมรู้ร่วมคิดเพื่อกู้คืนรหัสลับได้ แบบแผนที่ไม่ได้รับผลกระทบจากข้อจำกัดนี้กล่าวกันว่าปลอดภัยจากเสียงข้างมากที่ไม่ซื่อสัตย์ตามที่กล่าวไว้ในส่วนที่ 5.2 แพลตฟอร์มข้ามเชนต้องเพิ่มความปลอดภัยสูงสุดของเชนและสามารถทนต่อฝ่ายทุจริตให้ได้มากที่สุด ดังนั้น อุบายที่สามารถทนต่อความไม่ซื่อสัตย์ได้ส่วนใหญ่มีความจำเป็น

การลงนามล่วงหน้าการลงนามออนไลน์แบบไม่โต้ตอบ ในความพยายามที่จะลดภาระในการสื่อสารให้ฝ่ายต่างๆ ลงนามในข้อความ โปรโตคอลล่าสุดหลายฉบับได้ระบุส่วนสำคัญของงานสำหรับลายเซ็นที่สามารถทำได้ "ออฟไลน์" ก่อนที่ข้อความที่จะเซ็นจะเป็นที่รู้จัก [18, 13]. เอาต์พุตของเฟสออฟไลน์นี้เรียกว่าการลงนามล่วงหน้า การผลิตลายเซ็นล่วงหน้าถูกมองว่าเป็นโปรโตคอลที่แยกจากกัน T.Presign ซึ่งแตกต่างจาก T.Keygen และ T.Sign ผลลัพธ์ของโปรโตคอลการลงนามล่วงหน้าจะต้องถูกเก็บไว้เป็นส่วนตัวโดยฝ่ายต่างๆ จนกว่าจะใช้ในขั้นตอนการลงนาม

ต่อมาเมื่อทราบข้อความที่จะเซ็น งาน "ออนไลน์" เพิ่มเติมอีกเพียงเล็กน้อยเท่านั้นที่ต้องทำใน T.Sign เพื่อให้ลายเซ็นสมบูรณ์ ขั้นตอน T.Sign ออนไลน์ไม่ต้องการการสื่อสารระหว่างคู่สัญญา แต่ละฝ่าย ง่ายๆ ทำการคำนวณเฉพาะที่เกี่ยวกับข้อความและลายเซ็นล่วงหน้า จากนั้นจึงประกาศ si ส่วนแบ่งของลายเซ็น (เมื่อเป็นสาธารณะ ลายเซ็นเหล่านี้แชร์ s1, ... , st+1 จะถูกรวมโดยใครก็ตามเพื่อเปิดเผยลายเซ็นที่แท้จริง) คุณสมบัตินี้เรียกว่าการลงนามออนไลน์แบบไม่โต้ตอบ

ความแข็งแรงทนทาน แบบแผนเกณฑ์รับประกันเฉพาะกลุ่มย่อยของผู้ประสงค์ร้ายไม่สามารถเซ็นข้อความหรือเรียนรู้รหัสลับ อย่างไรก็ตาม การรับประกันนี้ไม่ได้กีดกันความเป็นไปได้ที่ผู้กระทำความผิด จะทำได้ปิดกั้นไม่ให้ทุกคนสร้างคีย์หรือลายเซ็น ในรูปแบบบางอย่างพฤติกรรมที่เป็นอันตรายโดยแม้ฝ่ายเดียวอาจทำให้ T.Keygen หรือ T.Sign ยกเลิกโดยไม่มีผลลัพธ์ที่เป็นประโยชน์ ทางเดียวคือรีสตาร์ทโปรโตคอล อาจเป็นกับฝ่ายอื่นสำหรับเซนแบบกระจายอำนาจ เราต้องการให้ T.Keygen และ T.Sign ประสบความสำเร็จหากอย่างน้อย t + 1 ของฝ่ายต่าง ๆ มีความซื่อสัตย์แม้ว่าบุคคลที่เป็นอันตรายบางรายจะส่งข้อความที่ผิดรูปแบบหรือส่งข้อความในโปรโตคอล คุณสมบัตินี้เรียกว่า *ความทนทาน*

การระบุแหล่งที่มาของความผิดพลาด ความสามารถในการระบุตัวแสดงที่ไม่ดีใน T.Keygen หรือ T.Sign เรียกว่าการระบุแหล่งที่มาของความผิดพลาด หากไม่มีการระบุแหล่งที่มาของข้อผิดพลาดเป็นการยากที่จะยกเว้นหรือลงโทษผู้กระทำผิดอย่างน่าเชื่อถือ ซึ่งในกรณีนี้ทุกคนจะต้องรับผิดชอบค่าใช้จ่ายที่เรียกเก็บโดยผู้กระทำผิด คุณสมบัตินี้ยังมีความสำคัญสำหรับเซนแบบกระจายศูนย์ซึ่งพฤติกรรมที่เป็นอันตรายควรสามารถระบุตัวตนได้และไม่ได้รับแรงจูงใจทางเศรษฐกิจผ่านกฎการฟันธง

ความปลอดภัยในการตั้งค่าพร้อมกัน โครงร่างลายเซ็นจะต้องปลอดภัยในการตั้งค่าพร้อมกัน โดยที่คีย์เจนและอัลกอริทึมการเซ็นชื่อหลายอินสแตนซ์สามารถเกี่ยวข้องพร้อมกันได้ (ตัวอย่างเช่น Drijvers et al. [16] แสดงการโจมตีแผนงานหลายลายเซ็นของ Schnorr ในการตั้งค่าเหล่านี้) มีทั้งแบบแผน ECDSA และ Schnorr ที่ตรงตามคุณสมบัติเหล่านี้ [13, 22]

ECDSA และ EdDSA เป็นรูปแบบลายเซ็นที่ปรับใช้กันอย่างแพร่หลายที่สุดในพื้นที่บล็อกเชนดังนั้นรุ่นธรณีประตูของทั้งสองแผนจึงเป็นจุดสนใจของการฟื้นตัวล่าสุดในการวิจัยและการพัฒนา. ผู้อ่านที่สนใจในความล้ำสมัยสามารถอ้างถึง [22, 13, 18] และรายงานการสำรวจล่าสุด [12]

5. Axelar Network

5.1. การออกแบบเชน Open Cross-Chain

สะพานที่เชน Axelar ดูแลรักษานั้นได้รับการสำรองข้อมูลโดยบัญชีเกณฑ์ ดังนั้น (เกือบ) ผู้ตรวจสอบความถูกต้องทั้งหมดต้องอนุญาตคำขอข้ามเชนทั้งหมดรวมกัน การออกแบบเชนที่ใครก็เข้าร่วมได้เพื่อรักษาความปลอดภัยสะพานเหล่านี้ต้องเป็นไปตามข้อกำหนดทางเทคนิคต่อไปนี้:

- *เปิดรับสมาชิก* ผู้ใช้ทุกคนควรสามารถเป็นผู้ตรวจสอบความถูกต้องได้ (ตามกฎของเชน)
- *อัพเดทการเป็นสมาชิก* เมื่อผู้ตรวจสอบออกจากระบบโดยสุจริต กุญแจจะต้องถูกเพิกถอนอย่างเหมาะสม
- *สิ่งจูงใจและการเชือด* ผู้ตรวจสอบความถูกต้องที่เป็นอันตรายควรสามารถระบุตัวตนได้ และการดำเนินการจะต้องระบุและแก้ไขโดยโปรโตคอล
- *ฉันทามติ* โครงร่างเกณฑ์กำหนดด้วยตัวเองเป็นโปรโตคอลแบบสแตนด์อโลน ในการเผยแพร่ข้อความระหว่างโหนด เราจำเป็นต้องมีทั้งช่องสัญญาณออกอากาศและช่องส่วนตัวแบบจุดต่อจุด นอกจากนี้ เครื่องมือตรวจสอบความถูกต้อง จำเป็นต้องเห็นด้วยกับสถานะล่าสุดของการเรียกใช้โครงร่างธรณีประตูแต่ละครั้งเนื่องจากมักจะมีหลายรายการรอบของการโต้ตอบ
- *การจัดการคีย์* เช่นเดียวกับผู้ตรวจสอบความถูกต้องทั่วไปในระบบ PoS ใด ๆ ที่ต้องปกป้องคีย์ของตนอย่างระมัดระวัง ดังนั้นผู้ตรวจสอบความถูกต้องของ Axelar จะต้องปกป้องส่วนแบ่งตามเกณฑ์ของตนเช่นกัน ต้องหมุนคีย์ แยกระหว่างส่วนออนไลน์และออฟไลน์ ฯลฯ

Axelar เริ่มต้นด้วยรูปแบบ Proof-of-Stake ที่ได้รับมอบสิทธิ์ซึ่งชุมชนเลือกชุดของผู้ตรวจสอบเพื่อเรียกใช้ฉันทามติ โปรดทราบว่ารูปแบบเกณฑ์มาตรฐานปฏิบัติต่อผู้เล่นทุกคนเหมือนกันและไม่มีความคิดเรื่อง "น้ำหนัก" ในฉันทามติ ดังนั้นเชนจะต้องปรับให้พวกเขาคำนึงถึงน้ำหนักของผู้ตรวจสอบ วิธีง่ายๆคือการกำหนดหุ้นเกณฑ์หลายตัวให้กับผู้ตรวจสอบที่ใหญ่กว่า ด้านล่างเป็นฟังก์ชันพื้นฐานสามฟังก์ชันที่ตัวตรวจสอบดำเนินการโดยรวม

- *เกณฑ์การสร้างคีย์ อัลกอริธึมการสร้างคีย์ขีดจำกัดที่มีอยู่สำหรับบล็อคเชนมาตรฐาน*รูปแบบลายเซ็น (ECDSA, Ed25519) เป็นโปรโตคอลแบบโต้ตอบระหว่างผู้เข้าร่วมหลายคน (ดูมาตรา 4). ธุรกรรมพิเศษบนเชน Axelar สั่งให้ผู้ตรวจสอบความถูกต้องเริ่มดำเนินการของโปรโตคอลแบบเก็บสถานะนี้ เครื่องมือตรวจสอบแต่ละตัวรันกระบวนการ threshold daemon ที่รับผิดชอบการรักษาความมั่นคงของรัฐที่เป็นความลับสำหรับแต่ละขั้นตอนของโปรโตคอล:
    1. เครื่องมือตรวจสอบจะเก็บสถานะของโปรโตคอลไว้ในหน่วยความจำภายในเครื่อง
    2. มันเรียกฎตลับเพื่อสร้างข้อความตามคำอธิบายโปรโตคอลสำหรับตัวตรวจสอบความถูกต้องอื่น
    3. มันเผยแพร่ข้อความผ่านการออกอากาศหรือผ่านช่องทางส่วนตัวไปยังผู้ตรวจสอบอื่น ๆ

4. เครื่องมือตรวจสอบแต่ละเครื่องจะเรียกใช้ฟังก์ชันการเปลี่ยนสถานะเพื่ออัปเดตสถานะดำเนินการขั้นตอนต่อไปของโปรโตคอล และทำซ้ำขั้นตอนข้างต้น

ที่ส่วนท้ายของโปรโตคอล คีย์สาธารณะของขีดจำกัดจะถูกสร้างขึ้นบน Axelar chain และสามารถแสดงกลับไปยังผู้ใช้ (เช่น สำหรับการฝากเงิน) หรือไปยังแอปพลิเคชันที่สร้างคำขอเริ่มต้น

- *เกณฑ์การลงนาม* คำขอลงนามบนเชน Axelar ได้รับการประมวลผลคล้ายกับคำขอสร้างคีย์ สิ่งเหล่านี้ถูกเรียกใช้ ตัวอย่างเช่น เมื่อผู้ใช้ต้องการถอนสินทรัพย์ออกจากเชนใดเชนหนึ่ง เหล่านี้เป็นโปรโตคอลแบบโต้ตอบ และการเปลี่ยนสถานะระหว่างรอบจะถูกทริกเกอร์ตามหน้าที่ของข้อความที่เผยแพร่ผ่านมุมมองบล็อกเชนของ Axelar และหน่วยความจำในเครื่องของผู้ตรวจสอบทุกคน
- *การจัดการการเปลี่ยนแปลงการเป็นสมาชิกของ Validator* ชุดตรวจสอบต้องหมุนเวียนเป็นระยะ เพื่อให้ผู้มีส่วนได้ส่วนเสียใหม่เข้าร่วมชุดได้ เมื่ออัปเดตชุดตัวตรวจสอบความถูกต้อง เราต้องอัปเดตคีย์ขีดจำกัดเพื่อแชร์ในชุดใหม่ ดังนั้น หากเราอนุญาตให้ใครก็ตามเข้าร่วมได้ทุกเมื่อ เราจะต้องอัปเดตคีย์ขีดจำกัดบ่อยมาก เพื่อป้องกันสิ่งนี้ เราหมุนเครื่องมือตรวจสอบทุกบล็อก *T* ภายในช่วงเวลา *T* รอบ *V^R* ที่ตั้งไว้และคีย์เกณฑ์จะได้รับการแก้ไข ในทุกรอบที่เป็นอินทิกรัลทวีคูณของพารามิเตอร์ *T* เราจะอัปเดตชุดเครื่องมือตรวจสอบดังนี้:
    1. ในทุกรอบ *R* สถานะ Axelar จะคอยติดตามชุดเครื่องมือตรวจสอบความถูกต้องปัจจุบัน *V^R. V^R+1 = V^R* เว้นแต่ *R + 1* เป็นทวีคูณของ *T*
    2. ระหว่างรอบ *((i - 1)T, iT]* ผู้ใช้โพสต์ข้อความเชื่อมโยง/ยกเลิกการผูกมัด
    3. เมื่อสิ้นสุดรอบ *iT* ข้อความเหล่านี้จะถูกนำไปใช้กับ *V^iT-1* เพื่อรับ *V^iT*
- *การสร้างคีย์ตามเกณฑ์และการลงนามต่อหน้าผู้ตรวจสอบความถูกต้องแบบหมุนเวียน* Axelar blockchain อาจออกคำขอสำหรับคีย์ใหม่หรือลายเซ็นขีดจำกัดที่รอบ *R* กระบวนการลงนามใช้เวลานานกว่าหนึ่งรอบ และเราไม่ต้องการชะลอการลงมติ เราจึงขอให้สร้างลายเซ็นก่อนรอบ *R + 10* เริ่ม. โดยเฉพาะอย่างยิ่ง ผู้ตรวจสอบความถูกต้องจะเริ่มรอบ *R + 10* หลังจากเห็นใบรับรองสำหรับรอบ *R + 9* และลายเซ็นสำหรับคำขอคีย์เจน/ลายเซ็นแต่ละรายการที่ออกในรอบ *R* ผลลัพธ์ของคำขอ *R* ทุกรอบจะต้องรวมอยู่ในบล็อก *R + 11* ใน กล่าวอีกนัยหนึ่ง ข้อเสนอบล็อก Round R ที่ไม่มีผลลัพธ์จากรอบ *R -11* ถือว่าไม่ถูกต้อง และผู้ตรวจสอบจะไม่ลงคะแนน เพื่อให้แน่ใจว่าข้อความขีดจำกัดทั้งหมดได้รับการ ลงนามก่อนการอัปเดตชุดเครื่องมือตรวจสอบความถูกต้อง Axelar จะไม่ออกคำขอขีดจำกัดใดๆ ระหว่างรอบที่เท่ากับ *-1, -2, . . , -9 โมดูโล T*

5.2. ความปลอดภัยของเชน

ความปลอดภัยของระบบบล็อคเชนนั้นขึ้นอยู่กับโปรโตคอลการเข้ารหัสและทฤษฎีเกมที่หลากหลาย รวมถึงการกระจายอำนาจของเชน ตัวอย่างเช่น ในบล็อกเชนแบบพิสูจน์การมีส่วนได้ส่วนเสีย

หากไม่มีผู้ตรวจสอบสิ่งจูงใจที่เหมาะสม อาจสมรู้ร่วมคิดและเขียนประวัติศาสตร์ใหม่โดยขโมยเงินของผู้ใช้รายอื่นในกระบวนการ ในเชนการพิสูจน์การทำงาน หากไม่มีการกระจายอำนาจที่เพียงพอ มันค่อนข้างง่ายที่จะสร้างส้อมยาวและใช้จ่ายสองเท่า เนื่องจากการโจมตีหลายครั้งบน Bitcoin Gold และ Ethereum Cla(S)sic ได้รับการพิสูจน์แล้ว

การวิจัยเกี่ยวกับความปลอดภัยของบล็อคเชนส่วนใหญ่มุ่งเน้นไปที่เชนอธิปไตย แต่เมื่อโซ่ทำงานร่วมกันจะต้องพิจารณาเวกเตอร์การโจมตีใหม่ ตัวอย่างเช่น สมมติว่า Ethereum พูดคุยกับบล็อคเชน X ขนาดเล็กผ่านสะพานตรงที่ควบคุมโดยสัญญาอัจฉริยะสองสัญญา สัญญาหนึ่งบน Ethereum และอีกหนึ่งใน X นอกจากความท้าทายด้านวิศวกรรมที่เราสรุปไว้ในส่วนที่ 1.1 เราต้องตัดสินใจว่าจะเกิดอะไรขึ้นเมื่อสมมติฐานความน่าเชื่อถือของ X ถูกละเมิด ในกรณีนี้ หาก ETH ย้ายไปที่ X ผู้ตรวจสอบความถูกต้องของ X อาจสมรู้ร่วมคิดเพื่อปลอมแปลง a

ประวัติของ X ที่พวกเขาถือ ETH ทั้งหมด โพสต์หลักฐานยืนยันที่เป็นเอกฉันท์ปลอมบน Ethereum และขโมย ETH สถานการณ์ยิ่งแย่ลงไปอีกเมื่อ X เชื่อมต่อกับเชนอื่นๆ หลายสายผ่านบริดจ์โดยตรง ซึ่งถ้า X แยกเอฟเฟกต์จะแพร่กระจายไปทั่วทุกบริดจ์ การกำหนดแนวทางการกำกับดูแลการกู้คืนสำหรับสะพานคู่แต่ละอันเป็นงานที่หนักหนาสาหัสสำหรับแต่ละโครงการ

เชน Axelar จัดการกับปัญหาด้านความปลอดภัยโดยใช้กลไกต่อไปนี้:

- *ความปลอดภัยสูงสุด* Axelar กำหนดเกณฑ์ความปลอดภัยไว้ที่ 90% ซึ่งหมายความว่าผู้ตรวจสอบความถูกต้องเกือบทั้งหมดจะต้องสมรู้ร่วมคิดเพื่อถอนเงินใด ๆ ที่ถูกล็อคโดยเชนหรือปลอมแปลงหลักฐานของรัฐ(1) ในทางปฏิบัติ มีการสังเกตว่าตัวตรวจสอบ PoS มีเวลาทำงานที่สูงมาก (เกือบ 100%) โดยถือว่าพวกเขาได้รับแรงจูงใจอย่างเหมาะสม ดังนั้น เชน Axelar จะสร้างบล็อกได้แม้ว่าจะมีเกณฑ์สูงก็ตาม อย่างไรก็ตาม ในกรณีที่เกิดข้อผิดพลาดขึ้นบ่อยครั้งและเชนหยุดชะงัก เชนต้องการกลไกสำรองที่แข็งแกร่งเพื่อรีบูตระบบตามที่อธิบายไว้ถัดไป
- *การกระจายอำนาจสูงสุด* เนื่องจากเชนใช้โครงร่างลายเซ็นขีดจำกัด จำนวนผู้ตรวจสอบจึงอาจมีขนาดใหญ่ที่สุด เชนไม่ได้ถูกจำกัดด้วยจำนวนผู้ตรวจสอบ ความถูกต้องที่เราสามารถรองรับได้ข้อจำกัดในการทำธุรกรรมหรือค่าธรรมเนียม ที่จะเกิดขึ้นจากการใช้ลายเซ็นหลายลายเซ็นบนเชนต่างๆ ที่ความซับซ้อน (และค่าธรรมเนียม) เพิ่มขึ้นตามจำนวนผู้ตรวจสอบความถูกต้อง (2)
- *กลไกการถอยกลับที่แข็งแกร่ง* คำถามแรกที่ต้องแก้ไขในเชนที่มีเกณฑ์ความปลอดภัยสูงดังข้างต้นคือสิ่งที่เกิดขึ้นเมื่อเชนหยุดทำงาน สมมติว่าเชน Axelar หยุดทำงาน เราสามารถมีกลไกสำรองที่จะให้ผู้ใช้กู้คืนเงินได้หรือไม่? ไปยังที่อยู่แผงลอยที่อาจเกิดขึ้นใด ๆ ของเชน Axelar เอง แต่ละบัญชีสะพานข้ามเกณฑ์บน blockchain X ที่ผู้ตรวจสอบความถูกต้องของ Axelar ควบคุมโดยรวมมี "กุญแจปลดล็อกฉุกเฉิน" คีย์นี้สามารถแชร์ในหลายพันฝ่ายและอาจเป็นคีย์ที่กำหนดเองสำหรับ blockchain X ที่แชร์ในชุมชนของเชนนั้น ดังนั้น หากเชน Axelar

หยุดชะงัก คีย์นี้จะทำหน้าที่เป็นทางเลือกสำรองและเปิดใช้งานการกู้คืนสินทรัพย์ (ดูรายละเอียดเพิ่มเติมด้านล่าง)

- *การกระจายอำนาจสูงสุดของกลไกการถอยกลับ* กลไกสำรองนี้ประกอบด้วยชุดการกู้คืนสำรองของผู้ใช้ ซึ่งทุกคนสามารถเข้าร่วมได้โดยไม่มีค่าใช้จ่ายใดๆ ผู้ใช้เหล่านี้ไม่จำเป็นต้องออนไลน์ ใช้งานโหนดหรือประสานงานระหว่างกัน พวกเขาจะถูก "เรียกเข้าปฏิบัติหน้าที่" เท่านั้นหากเชน Axelar หยุดทำงานและไม่สามารถกู้คืนได้ ความปลอดภัยของเชนได้รับการปรับปรุงโดยเกณฑ์ที่สูงมากในชุดเครื่องมือตรวจสอบหลักและชุดการกู้คืนสำรองที่มีการกระจายอำนาจสูงสุด
- *การกำกับดูแลร่วมกัน* โปรโตคอลทั่วไปควบคุมเชน Axelar โดยรวมแล้ว ผู้ใช้สามารถโหวตได้ว่าควรสนับสนุนเชนใดผ่านเชนของตน เชนจะจัดสรรกองทุนรวมที่สามารถใช้เพื่อคืนเงินให้ผู้ใช้ในกรณีที่เกิดเหตุฉุกเฉินที่ไม่คาดคิด ซึ่งควบคุมผ่านโปรโตคอลการกำกับดูแลเช่นกัน

กลไกการรักษาความปลอดภัยต่างๆ มีการกล่าวถึงด้านล่าง

กลไกการถอยกลับ เมื่อ Axelar หยุดทำงานเนื่องจากธรณีประตูสูง "กุญแจปลดล็อคฉุกเฉิน" จะเข้าควบคุมเชน มีหลายวิธีในการสร้างอินสแตนซ์ของกุญแจปลดล็อคนี้ และบางเชน/แอปพลิเคชันอาจเลือกใช้รูปแบบอื่นสำหรับ "ชุดการกู้คืน" หรือเลือกไม่รับทั้งหมด (3):

- Option a. แบ่งปันคีย์ข้ามรากฐานของโครงการบล็อคเชนและบุคคลที่มีชื่อเสียงในชุมชน
- Option b. แบ่งปันระหว่างฝ่ายต่างๆ ที่ได้รับเลือกผ่านกลไก PoS ที่ได้รับมอบหมาย
- Option c. สำหรับบัญชีที่จัดการทรัพย์สินและข้อมูลสำหรับลูกโซ่/แอปพลิเคชัน X ให้แชร์คีย์ที่กำหนดเองกับผู้มีส่วนได้ส่วนเสีย/ผู้ตรวจสอบความถูกต้องของ X สมมติว่า X มีกลไกการกำกับดูแลอยู่แล้ว กลไกการกำกับดูแลเดียวกันสามารถนำมาใช้เพื่อกำหนดแนวทางการดำเนินการหาก Axelar หยุดชะงัก

ตอนนี้ จากข้อมูลประจำตัวของผู้ใช้การกู้คืนและกุญแจสาธารณะ โปรโตคอลง่ายๆ จะสร้างการแชร์ของคีย์การกู้คืนที่ไม่มีใครรู้ ยิ่งกว่านั้นผู้ใช้ชุดการกู้คืนไม่จำเป็นต้องออนไลน์จนกว่าจะถูกเรียกให้กู้คืนผ่านกลไกการกำกับดูแล ตามโปรโตคอลการสร้างคีย์แบบกระจายมาตรฐาน ตัวตรวจสอบ Axelar แต่ละตัวจะแบ่งปันค่าแบบสุ่ม รหัสลับการกู้คืนถูกสร้างขึ้นโดยการรวมค่าเหล่านี้ แทนที่จะทำการสรุปอย่างชัดเจน การแชร์ทั้งหมดจะถูกเข้ารหัสภายใต้กุญแจสาธารณะของผู้ใช้ที่กู้คืนแล้วเพิ่ม homomorphically (สิ่งนี้ถือว่าการเข้ารหัสแบบ homomorphic เพิ่มเติมและชั้นเพิ่มเติมของความรู้ที่เป็นศูนย์ซึ่งทั้งสองอย่างนี้สามารถหาได้ง่าย) ผลลัพธ์ของโปรโตคอลนี้คือ *RPK* คีย์สาธารณะสำหรับการกู้คืน และอาจมีการเข้ารหัสนับพัน (ภายใต้คีย์สาธารณะของผู้ใช้การกู้คืน) ของการแชร์ของคีย์ลับ *Enc,i(si)* ที่เกี่ยวข้องซึ่งแจกจ่ายให้กับเจ้าของ (เช่น โพสต์บนเชน)). สัญญา Axelar bridge มีตัวเลือกในการคืนทุนโดยใช้ *RPK* ภายใต้เงื่อนไขบางประการ สุดท้ายยังสามารถอัปเดตคีย์การกู้คืนนี้ และแม้กระทั่งเปลี่ยนชุดผู้ใช้ที่ถือหุ้นโดยไม่ต้องดำเนินการใดๆ จากผู้ถือหุ้นที่เข้าร่วม

หากห่วงโซ่ X ที่เชื่อมต่อกับ Axelar ขาด มีสองตัวเลือก:

- กำหนดขีดจำกัดมูลค่า USD ของสินทรัพย์ที่สามารถย้ายเข้า/ออกจาก X ในวันใดก็ได้ ดังนั้น X ที่เป็นอันตรายจึงสามารถขโมยทรัพย์สินเพียงเล็กน้อยที่เชื่อมโยงกับมันก่อนที่ผู้ตรวจสอบความถูกต้องของ Axelar จะตรวจพบสิ่งนี้และกลไกการกำกับดูแลจากสัญลักษณ์แสดงหัวข้อย่อยต่อไปนี้จะเริ่มขึ้น
- โมดูลการกำกับดูแลของ Axelar สามารถใช้เพื่อลงคะแนนว่าเกิดอะไรขึ้นในสถานการณ์เหล่านั้น ตัวอย่างเช่น หากมีข้อบกพร่องที่ไม่ร้ายแรงและชุมชนรีสตาร์ท X การกำกับดูแลของ Axelar สามารถกำหนดเพื่อรีสตาร์ทการเชื่อมต่อจากตำแหน่งที่เหลือ
- หาก ETH ย้ายไปที่ X คีย์การกู้คืน Ethereum แบบกำหนดเองสามารถระบุได้ว่าเกิดอะไรขึ้นกับสินทรัพย์ ETH

6. Cross-Chain Gateway Protocol (CGP)

ในส่วนนี้ เราจะอธิบายเกี่ยวกับโปรโตคอลเกตเวย์ข้ามเชนและกลไกการกำหนดเส้นทางบนตัวอย่างหลักสองตัวอย่างที่พบได้ทั่วไประหว่างความต้องการของแอปพลิเคชันจำนวนมาก:

การซิงโครไนซ์สถานะ (ส่วนที่ 6.2) โพสต์ข้อมูลเกี่ยวกับสถานะของแหล่ง blockchain S ลงในสถานะของปลายทาง blockchain D

(เช่น โพสต์หัวข้อบล็อก Bitcoin ไปยัง Ethereum blockchain)

การโอนทรัพย์สิน (ส่วนที่ 6.3) โอนสินทรัพย์ดิจิทัลจาก S เป็น D แล้วกลับมาอีกครั้ง

(ตัวอย่างเช่น โอน bitcoins จาก Bitcoin blockchain ไปยัง Ethereum blockchain แล้วกลับไปที่ Bitcoin blockchain)

เพื่อความง่าย เราคิดว่า chain D นั้นรองรับ smart contract อย่างน้อยที่สุด แต่ S สามารถเป็น blockchain อะไรก็ได้

6.1. บัญชีในเชนอื่น

เพื่อเชื่อมโยงห่วงโซ่ที่แตกต่างกัน บัญชีเกณฑ์จะถูกสร้างขึ้นในแต่ละห่วงโซ่ ที่ควบคุมการไหล ของมูลค่าและข้อมูลข้ามพวกเขา สำหรับ chain(Chain) ให้ระบุบัญชีโดย Chain(Axelar)

บัญชี Bitcoin สำหรับ Bitcoin และสายสัญญาที่ไม่ฉลาดอื่น ๆ โปรแกรมตรวจสอบ Axelar จะสร้างคีย์ ECDSA ที่มีเกณฑ์ตามหัวข้อ 5.1 คีย์นี้ควบคุมบัญชี ECDSA บน Bitcoin และเป็นที่อยู่ปลายทางที่ผู้ใช้ฝากเงิน อาจมีการสร้างคีย์เกณฑ์ส่วนบุคคลตามคำขอของผู้ใช้ คีย์อาจได้รับการปรับปรุงเป็นระยะ และคีย์ล่าสุดและคีย์ส่วนบุคคลสามารถค้นหาได้โดยการสอบถามโหนด Axelar

บัญชีสะพานเกณฑ์บนเครือข่ายที่มีสัญญาอัจฉริยะ ระบุห่วงโซ่โดย คช. เครื่องมือตรวจสอบจะสร้างคีย์ ECDSA หรือ ED25519 เกณฑ์ตามหัวข้อ 5.1 ขึ้นอยู่กับประเภทคีย์ที่เชนรองรับ เราระบุคีย์นี้โดย *PK(Axelar)* เมื่อไม่มีความกำกวมว่าเราหมายถึงสายใด คีย์นี้ควบคุมบัญชีสัญญาอัจฉริยะบน *SC* ซึ่งแสดงโดย *SC(Axelar)* และแอปพลิเคชันใดๆ บน *SC* สามารถสอบถาม *SC(Axelar)* เพื่อเรียนรู้ที่อยู่ *PK* ของคีย์นั้น ด้วยวิธีนี้ แอปพลิเคชัน *SC* สามารถจดจำข้อความที่ลงนามโดย *SK(Axelar)* โปรโตคอลยังต้องพิจารณาถึงค่าการหมุนเวียนของ *PK(Axelar)* สิ่งนี้เกิดขึ้นดังนี้:

1. เริ่มต้น *SC(Axelar)* บน SC มันเก็บ *PK(Axelar)* ไว้เป็นส่วนหนึ่งของสถานะ ซึ่งเริ่มต้นตามค่ากำเนิดของมันบน Axelar *SC(Axelar)* ยังมีกฎสำหรับการอัปเดต *PK*
2. ในการอัปเดต *PK(Axelar)* จะต้องส่งธุรกรรมของรูปแบบ *(อัปเดต, PK(new))* พร้อมลายเซ็นจาก *SK(Axelar)* ปัจจุบัน จากนั้นสัญญากำหนด *PK(Axelar) = PK(new)*

3. ทุกครั้งที่ผู้ตรวจสอบอัปเดตคีย์ขีดจำกัดสำหรับ SC จาก *PKi* สำหรับ *PKi+1* Axelar ขอให้ผู้ตรวจสอบใช้ *SKi* เพื่อลงชื่อ *(อัปเดต PKi+1)* ต่อจากนั้นลายเซ็นนี้จะถูกโพสต์ไปยัง *SC(Axelar)* ซึ่งอัพเดต *PK(Axelar)*

6.2. การซิงโครไนซ์สถานะ

ให้ *q(S)* แสดงถึงคำถามตามอำเภอใจเกี่ยวกับสถานะของ chain S ตัวอย่างของคำถามดังกล่าว ได้แก่:

- "ในรอบบล็อกใด หากมีการทำธุรกรรม tx ปรากฏขึ้นหรือไม่"
- "ค่าของเขตข้อมูลหนึ่งมีค่าเท่าใด"
- "อะไรคือแฮชรูตของ Merkle ของสถานะ S ทั้งหมดที่บล็อกรอบ 314159?"

ให้ *a(S)* แสดงคำตอบที่ถูกต้องสำหรับ *q(S)* และสมมติว่าผู้ใช้ปลายทางหรือแอปพลิเคชันต้องการที่โพสต์ *a(S)* ไปยังเครือข่าย D. Axelar ตอบสนองความต้องการนี้ดังนี้:

1. ผู้ใช้โพสต์คำขอ *q(S)* บนหนึ่งในบัญชีบริดจ์ (ซึ่งจะถูกเลือกโดยผู้ตรวจสอบความถูกต้องในเวลาต่อมา) หรือส่งตรงไปยังบล็อกเชนของ Axelar
2. ในฐานะที่เป็นส่วนหนึ่งของฉันทามติของ Axelar ผู้ตรวจสอบความถูกต้องแต่ละคนต้องเรียกใช้ซอฟต์แวร์โหนดสำหรับเชน S, D ผู้ตรวจสอบความถูกต้องของ Axelar จะสอบถาม API ของซอฟต์แวร์โหนดลูกโซ่ S เพื่อหาคำตอบ *a(S)* และรายงานคำตอบไปยังห่วงโซ่ Axelar
3. เมื่อ > F เครื่องมือตรวจสอบแบบถ่วงน้ำหนักรายงานคำตอบเดียวกันที่รอบ R(Axelar) ขอให้ผู้ตรวจสอบความถูกต้องลงนาม *a(S)*
4. การใช้การเข้ารหัสขีดจำกัดตัวตรวจสอบความถูกต้องจะลงนามเป็น *a(S)* ลายเซ็นรวมอยู่ในบล็อก *R + 11*
5. ทุกคนสามารถนำค่าที่ลงนามเป็น *a(S)* จากบล็อก *R + 11* และโพสต์ไปที่ *D*
6. คำขอได้รับการบริการ แอปพลิเคชันใดๆ บน *D* อาจใช้ค่าที่ลงนามแล้ว *a(S)* เคียวรี *D(Axelar)* สำหรับ *PK(Axelar)* ล่าสุด และตรวจสอบว่าลายเซ็นของ *a(S)* สอดคล้องกับ *PK(Axelar)* ผู้ตรวจสอบความถูกต้องยังโพสต์ *a(S)* ไปยังบัญชีบริดจ์บน *chain D* ซึ่งแอปพลิเคชันสามารถดึงข้อมูลได้

6.3. การโอนสินทรัพย์ข้ามเครือข่าย

เครือข่ายช่วยให้สามารถถ่ายโอนสินทรัพย์ดิจิทัลข้ามเชนโดยขยายเวิร์กโฟลว์การซิงโครไนซ์สถานะของส่วนที่ 6.2

อุปทานที่เพียงพอของโทเค็น pegged-*S* ถูกพิมพ์และควบคุมโดย *D(Axelar)* เมื่อเริ่มต้น สมมติว่าผู้ใช้ต้องการแลกเปลี่ยนจำนวน x ของโทเค็นบนซอร์สเชน S สำหรับจำนวน x ของโทเค็น pegged-*S*

บนเชนปลายทาง *D* เพื่อฝากไว้ที่ *D-address w(D)* ที่ผู้ใช้เลือก เรานำเสนอเวิร์กโฟลว์ทั่วไปทั้งหมด ซึ่งรองรับซอร์สเชน S—แม้แต่เชนเช่น Bitcoin ที่ไม่รองรับ smartcontract:

1. ผู้ใช้ (หรือแอปพลิเคชันที่ดำเนินการในนามของผู้ใช้) โพสต์คำขอโอน *(x, w(D))* ไปยังบัญชีธรณีประตูบริดจ์ ซึ่งต่อมาจะถูกส่งไปยังเครือข่าย Axelar
2. ผู้ตรวจสอบความถูกต้องของ Axelar ใช้การเข้ารหัสตามเกณฑ์เพื่อสร้างที่อยู่ฝากใหม่ *d(S)* สำหรับ *S* โดยจะโพสต์ *d(S)* ไปยังบล็อกเชนของ Axelar
3. ผู้ใช้ (หรือแอปพลิเคชันที่ดำเนินการในนามของผู้ใช้) เรียนรู้ d(S) โดยการตรวจสอบ Axelar blockchain ผู้ใช้ส่ง S-token จำนวน x เพื่อจัดการกับ d(S) ผ่านธุรกรรม S ธรรมดา tx(S) โดยใช้ซอฟต์แวร์ที่เธอโปรดปรานสำหรับ chain S

   (เนื่องจากคุณสมบัติขีดจำกัดของ d(S) โทเค็นไม่สามารถใช้จาก d(S) ได้ เว้นแต่หมายเลขเกณฑ์ ของตัวตรวจสอบจะประสานงานให้ทำเช่นนั้น)

4. *tx(S)* ถูกโพสต์บน Axelar เครื่องมือตรวจสอบความถูกต้องจะสอบถาม API ของซอฟต์แวร์โหนด *S* ของลูกโซ่สำหรับการมีอยู่ของ *tx(S)* และหากการตอบสนองเป็น "จริง" ให้รายงานคำตอบไปยังห่วงโซ่ Axelar
5. เมื่อ > F ตัวตรวจสอบน้ำหนักที่รายงาน "จริง" สำหรับ *tx(S)* ที่รอบ *R*, Axelar ขอให้ผู้ตรวจสอบความถูกต้องลงนามในธุรกรรม *a(D)* ที่ส่งจำนวน x ของโทเค็นที่ pegged-*S* จาก *D(Axelar)* ไปยัง *w(D)*
6. การใช้การเข้ารหัสธรณีประตูผู้ตรวจสอบจะลงนามในโฆษณา ลายเซ็นรวมอยู่ในบล็อก *R + 11*
7. ทุกคนสามารถนำค่าลงนาม *a(D)* จากบล็อก *R + 11* และโพสต์ไปที่ *D*
8. คำขอได้รับบริการแล้ว เมื่อมีการโพสต์โฆษณาบน *D* การโอนจะได้รับการดำเนินการ

ในตอนนี้ สมมติว่าผู้ใช้ต้องการแลกใช้จำนวน x' ของ wrapped-*S* จากสาย *D* กลับไปยังสาย *S* เพื่อฝากไว้ที่ *S*-address w(S) ที่ผู้ใช้เลือก เวิร์กโฟลว์มีดังนี้:

1. ผู้ใช้เริ่มต้นคำขอโอน *(x', w(S))* โดยการฝากโทเค็นห่อหุ้ม *S* จำนวน *x'* ลงใน *c(D)* ผ่านธุรกรรม *D* ธรรมดาโดยใช้ซอฟต์แวร์ที่เธอโปรดปรานสำหรับเชน *D*
2. *(x', w(S))* ถูกโพสต์บน Axelar เครื่องมือตรวจสอบความถูกต้องจะสอบถาม API ของซอฟต์แวร์โหนด chain *D* สำหรับการมีอยู่ของ *(x', w(S))* และหากการตอบสนองเป็น "จริง" ให้รายงานคำตอบไปยัง Axelar chain

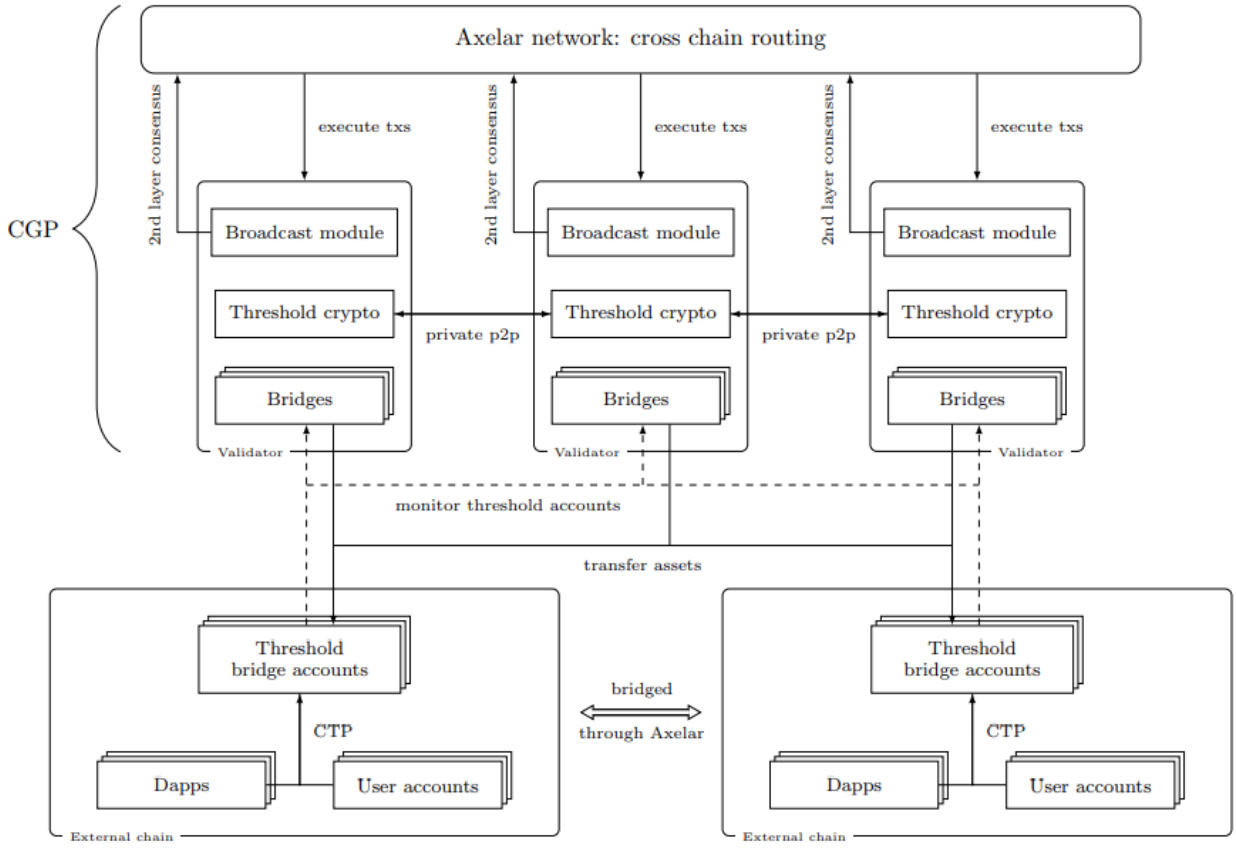

Figure 1 แผนภาพส่วนประกอบ

3. เมื่อ > F ตัวตรวจสอบน้ำหนักรายงาน "จริง" สำหรับ *(x ', w (S))* ที่รอบ *R(Axelar)* ขอให้ผู้ตรวจสอบความถูกต้องลงนามในธุรกรรม *a(S)* ที่ส่งโทเค็น *S* จำนวน *x'* จาก *S(Axelar)* ไปยัง *w(S)*
4. การใช้การเข้ารหัสขีดจำกัดตัวตรวจสอบความถูกต้องจะลงนามเป็น *a(S)* ลายเซ็นรวมอยู่ในบล็อก *R + 11*
5. ทุกคนสามารถนำค่าที่ลงนามเป็น *a(S)* จากบล็อก *R + 11* และโพสต์ไปที่ *S*
6. คำขอได้รับบริการแล้ว เมื่อมีการโพสต์ *a(S)* บน *S* การโอนจะได้รับการดำเนินการ

คำขอเพิ่มเติมที่สนับสนุนโดยเลเยอร์การกำหนดเส้นทาง CGP รวมถึงการล็อก การปลดล็อก หรือการโอนสินทรัพย์ข้ามเครือข่าย

บรรลุโฟลว์ธุรกรรมข้ามสายของอะตอมขึ้นอยู่กับประเภทคำขอข้าม เช่น Axelar พยายามทำให้แน่ใจว่าธุรกรรมที่เกี่ยวข้องนั้นถูกดำเนินการบนหลายสายหรือไม่มีเลย ในการนี้ ทุกคำขอสามารถอยู่ในสถานะใดสถานะหนึ่งต่อไปนี้ใน Axelar blockchain: (เริ่มต้น, รอดำเนินการ, เสร็จสมบูรณ์, หมดเวลา) หากมีการทริกเกอร์การหมดเวลาในขั้นตอนที่รอดำเนินการ คำขอจะส่งกลับรหัสข้อผิดพลาด เหตุการณ์การหมดเวลาบางเหตุการณ์ยังเริ่มต้นเหตุการณ์การคืนเงินด้วย: ตัวอย่างเช่น หากจำเป็นต้องโอนสินทรัพย์จากห่วงโซ่หนึ่งไปยังสินทรัพย์ในอีกสายหนึ่ง หากห่วงโซ่การรับไม่ดำเนินการธุรกรรม ทรัพย์สินจะถูกส่งคืนกลับไปยังผู้ใช้เดิม

7. Cross-Chain Transfer Protocol (CTP)

CTP เป็นโปรโตคอลระดับแอปพลิเคชันที่ช่วยให้แอปพลิเคชันใช้ประโยชน์จากคุณลักษณะข้ามเชนได้ง่าย เราอธิบายการผสานรวมโดยเน้นที่คุณสมบัติการโอนสินทรัพย์ (เช่น ใช้ใน DeFi) โดยทั่วไปแล้ว แอปพลิเคชันเหล่านี้ประกอบด้วยสามองค์ประกอบหลัก ได้แก่ GUI ส่วนหน้า, สัญญาอัจฉริยะในสายเดียว และโหนดตัวกลางที่โพสต์ธุรกรรมระหว่างส่วนหน้าและสัญญาอัจฉริยะ ส่วนหน้าโต้ตอบกับกระเป๋าเงินของผู้ใช้เพื่อรับเงินฝาก ดำเนินการถอนเงิน ฯลฯ แอปพลิเคชันสามารถใช้ประโยชน์จากคุณสมบัติข้ามเชน 12 โดยการเรียกแบบสอบถาม CTP ที่คล้ายคลึงกับวิธี HTTP/HTTPS GET/POST คิวรีเหล่านี้จะถูกเลือกในภายหลังโดยเลเยอร์ CGP สำหรับการดำเนินการและผลลัพธ์จะถูกส่งกลับไปยังผู้ใช้

- *CTP Queries* นักพัฒนาแอปพลิเคชันสามารถโฮสต์แอปพลิเคชันของตนบนเครือข่ายใดก็ได้ และผสานรวมสมาร์ทคอนแทรคกับบัญชีขีดจำกัดของบริดจ์เพื่อดำเนินการสืบค้น CTP
- *บัญชีข้ามเกณฑ์* สมมติว่านักพัฒนาแอปพลิเคชันสร้างสัญญาของตนในสาย A จากนั้นพวกเขาจะอ้างอิงสัญญาสะพานข้ามเพื่อรับการสนับสนุนข้ามสาย สัญญานี้อนุญาตให้แอปพลิเคชัน:
  - ลงทะเบียน blockchain ที่ต้องการสื่อสารด้วย
  - ลงทะเบียนสินทรัพย์บนบล็อคเชนที่ต้องการใช้ประโยชน์
  - ดำเนินการกับสินทรัพย์ เช่น รับเงินฝาก ดำเนินการถอนเงิน และหน้าที่อื่นๆ (คล้ายกับการเรียกตามสัญญา ERC-20)

สมมติว่า MapleSwap แอปพลิเคชั่น DeFi ที่โดดเด่นซึ่งอยู่ในการลงทะเบียนลูกโซ่ A กับบัญชีธรณีประตูผู้ตรวจสอบความถูกต้องของ Axelar จะจัดการสัญญาเองในห่วงโซ่ที่เกี่ยวข้อง สมมติว่าผู้ใช้ต้องการฝากเงินเข้าในคู่ซื้อขายระหว่างสินทรัพย์ X และ Y ที่อยู่ในสองเครือข่ายตามลำดับ จากนั้น เมื่อผู้ใช้ส่งคำขอดังกล่าว คำขอนั้นจะถูกส่งผ่านบัญชี Threshold Bridge ไปยังเครือข่าย Axelar เพื่อดำเนินการ แบบฟอร์มมีการดำเนินการตามขั้นตอนต่อไปนี้:

1. เครือข่าย Axelar เข้าใจดีว่าแอปพลิเคชันนี้ลงทะเบียนสำหรับการสนับสนุนข้ามเชนทั่วทั้งสินทรัพย์ มันสร้างคีย์การฝากเงินที่ใช้ประโยชน์จากการเข้ารหัสตามเกณฑ์และความเห็นพ้องต้องกันสำหรับผู้ใช้ในเชน A และ B ที่สอดคล้องกัน
2. กุญแจสาธารณะที่เกี่ยวข้องจะถูกส่งกลับไปยังแอปพลิเคชันและแสดงต่อผู้ใช้ที่สามารถใช้กระเป๋าเงินที่พวกเขาชื่นชอบในการฝากเงินได้ รหัสลับที่เกี่ยวข้องจะถูกแชร์กับตัวตรวจสอบ Axelar ทั้งหมด
3. เมื่อเงินฝากได้รับการยืนยัน Axelar จะอัปเดตไดเร็กทอรี cross-chain เพื่อบันทึกว่าผู้ใช้ใน chain ที่เกี่ยวข้องได้ฝากสินทรัพย์เหล่านี้
4. ตัวตรวจสอบความถูกต้องของ Axelar เรียกใช้โปรโตคอลหลายฝ่ายเพื่อสร้างลายเซ็นขีดจำกัดที่อนุญาตให้อัปเดตบัญชีบริดจ์ของขีดจำกัดบนเชน A ที่แอปพลิเคชันตั้งอยู่

5. จากนั้นเคียวรี CTP จะถูกส่งกลับไปยังสัญญาอัจฉริยะของแอปพลิเคชัน DeFi ซึ่งสามารถอัปเดตสถานะ อัปเดตสูตรผลตอบแทน อัตราแลกเปลี่ยน หรือดำเนินการตามเงื่อนไขอื่นๆ ที่เกี่ยวข้องกับสถานะของแอปพลิเคชัน

ตลอดกระบวนการนี้ เครือข่าย Axelar ในระดับสูงทำหน้าที่เป็นออราเคิลการอ่าน/เขียนข้ามเชนที่กระจายอำนาจ CGP เป็นเลเยอร์การกำหนดเส้นทางระหว่างเชน และ CTP เป็นโปรโตคอลแอปพลิเคชัน

คำขอข้ามเชนเพิ่มเติม CTP รองรับ cross-chain ทั่วไปมากขึ้นระหว่างแอปพลิเคชันต่างๆ ทั่ว blockchains เช่น:

- ดำเนินการบริการชื่อคีย์สาธารณะ (PKNS) นี่คือไดเร็กทอรีสากลสำหรับการแมปกุญแจสาธารณะกับหมายเลขโทรศัพท์/ตัวจัดการทวิตเตอร์ (บางโปรเจ็กต์ เช่น Celo มีคุณลักษณะเหล่านี้ภายในแพลตฟอร์มของพวกเขา)
- ทริกเกอร์แอปพลิเคชันข้ามสาย แอปพลิเคชันบน chain A สามารถอัปเดตสถานะได้หากแอปพลิเคชันอื่นใน chain B ตรงตามเกณฑ์การค้นหา (อัตราดอกเบี้ย < X)
- ความสามารถในการทำสัญญาที่ชาญฉลาด สัญญาอัจฉริยะบนเชน A สามารถอัปเดตสถานะตามสถานะของสัญญาในเชน B หรือทริกเกอร์การดำเนินการเพื่ออัปเดตสัญญาอัจฉริยะบนเชน B

ในระดับสูง คำขอเหล่านี้สามารถประมวลผลได้ตั้งแต่โดยรวม โปรโตคอล CTP, CGP และเครือข่าย Axelar สามารถส่งและเขียนข้อมูลสถานะที่ตรวจสอบได้โดยพลการในบล็อคเชน

8. Summary

ในอีกไม่กี่ปีข้างหน้า แอปพลิเคชันและทรัพย์สินที่สำคัญจะถูกสร้างขึ้นบนระบบนิเวศบล็อกเชนหลายแห่ง เครือข่าย Axelar สามารถใช้เพื่อเสียบบล็อกเชนเหล่านี้ลงในเลเยอร์การสื่อสารข้ามเชนที่สม่ำเสมอ เลเยอร์นี้จัดเตรียมโปรโตคอลการกำหนดเส้นทางและระดับแอปพลิเคชันที่ตอบสนองทั้งผู้สร้างแพลตฟอร์มและความต้องการของนักพัฒนาแอปพลิเคชัน นักพัฒนาแอปพลิเคชันสามารถสร้างบนแพลตฟอร์ม ที่ดีที่สุดสำหรับความต้องการของพวกเขา และใช้ประโยชน์จากโปรโตคอลและ API อย่างง่าย เพื่อเข้าถึงสภาพคล่องข้ามเชนทั่วโลก ผู้ใช้และสื่อสารกับเครือข่ายอื่นๆ

อ้างอิง

[1] Althea peggy. https://github.com/cosmos/peggy . [Cited on page 2.]

[2] Deterministic usage of the digital signature algorithm (dsa) and elliptic curve digital signature algorithm (ecdsa). https://tools.ietf.org/html/rfc6979 . [Cited on page 5.]

[3] Edwards-curve digital signature algorithm (eddsa). https://tools.ietf.org/html/rfc8032 . [Cited on page 5.]

[4] Eos.io technical white paper v2. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md . [Cited on page 1.]

[5] Ethereum: A secure decentralised generalised transaction ledger. https://ethereum.github.io/yellowpaper/paper.pdf . [Cited on page 1.]

[6] The near white paper. https://near.org/papers/the-official-near-white-paper/ . [Cited on page 1.]

[7] Rainbow bridge. https://github.com/near/rainbow-bridge . [Cited on page 2.]

[8] Ren: A privacy preserving virtual machine powering zero-knowledge financial applications. https://whitepaper.io/document/419/ren-litepaper . [Cited on page 3.]

[9] tbtc: A decentralized redeemable btc-backed erc-20 token. https://docs.keep.network/tbtc/index. pdf . [Cited on page 2.]

[10] Thorchain: A decentralized liquidity network. https://thorchain.org/ . [Cited on page 3.]

[11] Kurt M. Alonso. Zero to monero. https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf . [Cited on page 1.]

[12] Jean-Philippe Aumasson, Adrian Hamelink, and Omer Shlomovits. A survey of ecdsa threshold signing. Cryptology ePrint Archive, Report 2020/1390, 2020. https://eprint.iacr.org/2020/1390 . [Cited on page 6.]

[13] Ran Canetti, Nikolaos Makriyannis, and Udi Peled. Uc non-interactive, proactive, threshold ecdsa. Cryptology ePrint Archive, Report 2020/492, 2020. https://eprint.iacr.org/2020/492 . [Cited on page 6.]

[14] cLabs Whitepapers. https://celo.org/papers . [Cited on page 1.]

[15] Ivan Damg˚ard, Thomas Pelle Jakobsen, Jesper Buus Nielsen, Jakob Illeborg Pagter, and Michael Bæksvang Østerg˚ard. Fast threshold ECDSA with honest majority. In SCN, volume 12238 of Lecture Notes in Computer Science, pages 382–400. Springer, 2020. [Cited on page 6.]

[16] Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs. On the security of two-round multi-signatures. In IEEE Symposium on Security and Privacy, pages 1084–1101. IEEE, 2019. [Cited on page 6.] 14

[17] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf . [Cited on page 5.]

[18] Rosario Gennaro and Steven Goldfeder. One round threshold ecdsa with identifiable abort. Cryptology ePrint Archive, Report 2020/540, 2020. https://eprint.iacr.org/2020/540 . [Cited on page 6.]

[19] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. Proceedings of the 26th Symposium on Operating Systems Principles, 2017. https://dl.acm.org/doi/pdf/10.1145/3132747.3132757 . [Cited on page 1.]

[20] Evan Kereiakes, Do Kwon, Marco Di Maggio, and Nicholas Platias. Terra money: Stability and adoption. https://terra.money/Terra_White_paper.pdf . [Cited on page 1.]

[21] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. https://eprint.iacr.org/2016/889.pdf . [Cited on page 1.]

[22] Chelsea Komlo and Ian Goldberg. Frost: Flexible round-optimized schnorr threshold signatures. Cryptology ePrint Archive, Report 2020/852, 2020. https://eprint.iacr.org/2020/852 . [Cited on page 6.]

[23] Jae Kwon and Ethan Buchman. Cosmos: A network of distributed ledgers. https://cosmos.network/resources/whitepaper . [Cited on pages 1 and 2.]

[24] Avalanche Team. Avalanche platform. https://www.avalabs.org/whitepapers . [Cited on pages 1 and 2.]

[25] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. https://polkadot.network/PolkaDotPaper.pdf . [Cited on pages 1 and 2.]